Syllabus

Course Description

Course Title	Cybersecurity and Digital Privacy
Course Code	27525
Course Title Additional	
Scientific-Disciplinary Sector	GIUR-01/A
Language	English
Degree Course	Master in Data Analytics for Economics and Management
Other Degree Courses (Loaned)	
Lecturers	Prof. Laura Valle, Laura.Valle@unibz.it https://www.unibz.it/en/faculties/economics-management/academic-staff/person/11518 Mag.phil.Dr.iur. Christoph Perathoner, Christoph.Perathoner@unibz.it https://www.unibz.it/en/faculties/economics-management/academic-staff/person/40440
Teaching Assistant	
Semester	Second semester
Course Year/s	1
CP	3
Teaching Hours	- 12 hours of in-person lectures - 6 hours of video lectures (counted as 12 hours to account for re-watching)
Lab Hours	-
Individual Study Hours	-
Planned Office Hours	9, including 3 hours offered as virtual classroom sessions
Contents Summary	The course deals with the main legal issues on personal and non-personal data processing and the risk management that a cyber-company faces in the current European regulatory framework. In the first part of the course personal and non-personal data processing regulations will be studied. The GDPR's main provisions

	will be described, and then how the GDPR addresses the rules governing data processing and the duties cast upon controllers and processors. The role and obligations of Data Protection Officers (DPO) are dealt with. The comparative perspective among the EU legal model with the US legal model and the Chinese legal model of data processing and protection will be explored. The international level of rules formation in the field is also taken into account. The second part of the course focuses on cybersecurity. After the description of the main threats and vulnerabilities of networks, it focuses on the best practices and rules used to tackle them. It analyses the NIS Directive and the Cybersecurity Act in force into the European Union. It concludes with the discussion about how these rules are tailored within specific industries.
Course Topics	The course deals with the main legal issues on personal and non-personal data processing and about the risk management that a cyber-company faces. In the first part of the course personal and non-personal data processing regulations will be studied. The GDPR's main provisions will be described, its rules governing data processing and the duties cast upon controllers and processors. The role and general obligations of Data Protection Officers (DPO) are dealt with. The second part of the course deals with the basic elements of Cybersecurity with the aim to provide a comprehensive and structured overview of the main topics related to the discipline, addressing both technical and organizational as well as regulatory aspects. First, the course will examine the main threats and vulnerabilities affecting information systems, networks, and applications, with particular attention to the most widespread attack techniques and the ways in which they can compromise the confidentiality, integrity, and availability of information. It will then focus on the principles of risk governance, with the goal of understanding how organizations can adopt effective management strategies and how to conduct a proper risk assessment using internationally recognized methodologies. The course will also cover technical and organizational security measures and best practices aimed at mitigating risks, including security policies, access controls, encryption, and monitoring systems. A specific focus will be placed on the national and European regulatory landscape, with references to regulations and directives such as

	the NIS2 Directive, to understand legal implications and compliance requirements organizations must meet. The ultimate goal is to provide students with both theoretical and practical tools to critically and effectively face the challenges of Cybersecurity.
Keywords	Data processing, cybersecurity, data protection, data protection officer.
Recommended Prerequisites	NA
Propaedeutic Courses	
Teaching Format	Recorded lectures, in-person teaching, exercises. The course adopts a blended, student-centred approach that emphasises problem-based learning and active engagement. A portion of the lecture content is made available online in advance, allowing students to explore key concepts independently and at their own pace before attending class. This preparatory work enables inperson sessions to focus on the application of knowledge through real-world problems, collaborative activities, and guided discussions — fostering critical thinking and deeper learning. The course is fully aligned with the principles of the Italian Universities Digital Hub (EDUNEXT) initiative (https://edunext.eu), which promotes the integration of digital resources and active learning strategies within university teaching.
Mandatory Attendance	Attendance is recommended, but not mandatory.
Specific Educational Objectives and Learning Outcomes	Intended Learning Outcomes (ILO) ILO 1 Knowledge and understanding: ILO 1.1 The student acquires advanced knowledge of the legal aspects of data processing. ILO 1.2 The student develops knowledge and understanding of the legal aspects of privacy, the essential elements of data protection legislation, and the privacy risks arising from the release of data. ILO 1.3 The student develops knowledge and understanding of aspects related to data security, the cybercrime ecosystem, and vulnerabilities in companies and institutions in relation to cyber attacks. ILO 2 Applying knowledge and understanding:

	ILO 2.1 Ability to navigate the legal system with confidence in order to deal with common issues relating to data security and privacy. ILO 3 Making judgements: ILO 3.1 The student acquires the ability to apply acquired knowledge to interpret data in order to make directional and operational decisions in a business context. ILO 3.2 The student acquires the ability to apply acquired knowledge to support processes related to production, management and risk promotion activities and investment choices through the organisation, analysis and interpretation of complex databases. ILO4 Communication skills: ILO 4.1 The student acquires the ability to communicate effectively in oral and written form the specialised content of the individual disciplines, using different registers, depending on the recipients and the communicative and didactic purposes, and to evaluate the formative effects of his/her communication. ILO 5 Learning skills: ILO 5.1 The student acquires knowledge of scientific research tools. He/she will also be able to make autonomous use of information technology to carry out bibliographic research and investigations both for his/her own training and for further education. Furthermore, through the curricular teaching and the activities related to the preparation of the final thesis, she will be able to acquire the ability - to identify thematic connections and to establish relationships between methods of analysis and application contexts; - to frame a new problem in a systematic manner and to implement appropriate analysis solutions; - to formulate general statistical-econometric models from the phenomena studied.
Specific Educational Objectives and Learning	

Outcomes (additional info.)	
Assessment	The final exam consists of 3-4 written open questions with subquestions. (ILOs 1-5)
Evaluation Criteria	Criteria for the assessment of the written exam: clarity of the answers, mastery of language (knowledge of the legal technical language, and grammatical and logic mastery of language), ability to summarize, evaluate, and establishing relationships between topics.
Required Readings	- *Data protection in context: between privacy and AI*, ed. by E. Longo, A. Pin, F. Viglione, Giuffré, Milano, 2025. - Stallings and Brown, Computer Security: Principles and Practice, Global Edition, 5a ed., 2025. The chapters to prepare for the exam will be indicated in the detailed syllabus uploaded on Teams.
Supplementary Readings	
Further Information	
Sustainable Development Goals (SDGs)	Industry, innovation and infrastructure, Quality education